Sheet # 4
Hash Function, Access Control and Key Management

Exercises

1. A message is made of 10 numbers between 00 and 99. A hash algorithm creates a digest out of this message by adding all numbers modulo 100. The resulting digest is a number between 00 and 99. Does this algorithm meet the first criterion of a hash algorithm? Does it meet the second criterion? Does it meet the third criterion?
2. ***(Report)*** A message is made of 100 characters. A hash algorithm creates a digest out of this message by choosing characters 1, 11, 21... , and 91. The resulting digest has 10 characters. Does this algorithm meet the first criterion of a hash algorithm? Does it meet the second criterion? Does it meet the third criterion?
3. At a party, which is more probable, a person with a birthday on a particular day or two persons or more (at least two) having the same birthday? How is the solution related to the second and the third criteria of a hashing function? (Assume 10 guests).
4. A hash algorithm creates a digest of *N* bits. How many different digests can be created from this algorithm?
5. A message is 20,000 characters. We are using a digest of this message using SHA-l. After creating the digest, we decided to change the last 10 characters. Can we say how many bits in the digest will be changed?

6.

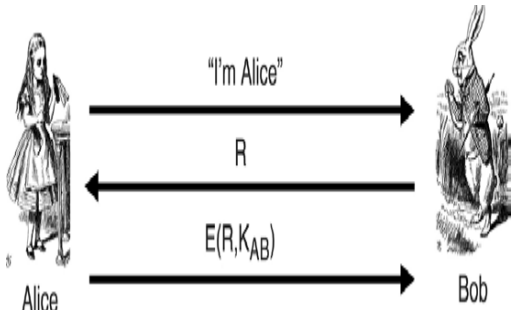

Fig.6a

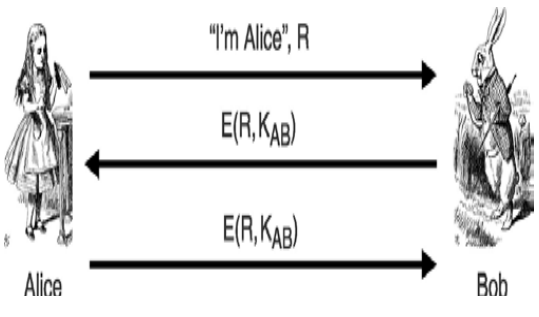

Fig6.b

a) *In Fig. 6a,* what is the type of this challenge? Explain briefly how it provides entity authentication.
b) Fig.6a only authenticates Alice to Bob. To obtain a mutual authentication, we suggest the solution in Fig.6b; do you think it will work? *Explain.*

Review Questions

1. What are some advantages and disadvantages of using long passwords?
2. We discussed fixed and one-time passwords as two extremes. What about frequently changed passwords? How do you think this scheme can be implemented? What are the advantages and disadvantages?
3. How can a system prevent a guessing attack on a password? How can a bank prevent PIN guessing if someone has found or stolen a bank card and tried to use it?
4. What is a nonce?
5. What is the N^2 problem?
6. Name a protocol that uses a KDC for user authentication.
7. What is the purpose of the Kerberos authentication server (AS)?
8. What is the purpose of the Kerberos ticket-granting server (TGS)?
9. What is the purpose of *X.509?*
10. What is a certification authority (CA)?

Best Wishes of Success